International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

# Blockchain-Based Agri-Food Supply Chain

**Nikita Khose, Mrs.Vaishali Hatkar**

***Dept of MCA-Trinity Academy of Engineering, Pune,India Assitant***

***Professor, Trinity Academy of Engineering, Pune,India***

## ABSTRACT

Supply chains are evolving into automated and highly complex networks and are becoming an important source of potential benefits in the modern world. At the same time, consumers are now more interested infood product quality. However, it is challenging to track the provenance of data and maintain itstraceability throughout the supply chain network. The traditional supply chains are centralized and they depend on a third party for trading. These centralized systems lack transparency, accountability and auditability. In our proposed solution, we have presented a complete solution for blockchain-based Agriculture and Food (Agri-Food) supply chain. It leverages the key features of blockchain and smart contracts, deployed over ethereum blockchain network. Although blockchain provides immutability of data and records in the network, it still fails to solve some major problems in supply chain management like credibility of the involved entities, accountability of the trading process and traceability of the products.

## I. INTRODUCTION

Block Chain Technology:
A block-chain is a database that is shared across a network of computers. Once a record has been added to the chain it is very difficult to change. The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain. The term ”block-chain technology” typically refers to the transparent, trustless, publicly accessible ledger that allows us to securely transfer the ownership of units of value using public key encryption and proof of work methods. The technology uses decentralized consensus to maintain the network, which means it is not centrally controlled by a bank, corporation, or government. In fact, the larger the network grows and becomes increasingly decentralized, the more secure it becomes. A block-chain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. Crowdsourcing is a sourcing model in which individuals or organizations obtain goods and services,including ideas and finances, from a large, relatively open and often rapidly-evolving group of internet users; it divides work between participants to achieve a cumulative result

## II. LITERATURE SURVEY/BACKGROUND

"New directions in cryptography" Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

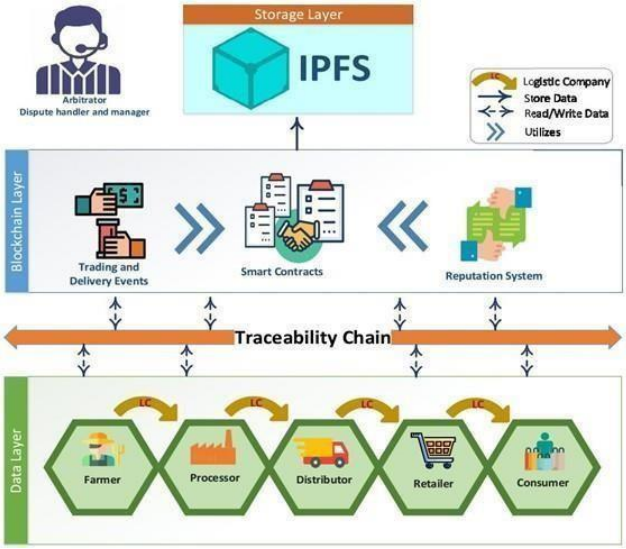
"An efficient protocol for authenticated key agreement" This paper proposes an efficient two-pass protocol for authenticated key agreement in the asymmetric (public-key) setting. The protocol is based on Diffie-Hellman key agreement and can be modified to work in an arbitrary finite group and, in particular, elliptic curve groups. Two modifications of this protocol are also presented: a one- pass authenticated key agreementprotocol suitable for environments where only one entity is on-line, and a three-pass protocol in which key confirmation is additionally provided. Variants of these protocols have been standardized in IEEE P1363, ANSI X9.42, ANSI X9.63 and ISO 15496-3, and are currently under consideration forstandardization and by the U.S. government's National Institute for Standards and Technology.

Identity-based fault-tolerant conference key agreement"Lots of conference key agreement protocols have been suggested to secure computer network conference. Most of them operate only when all conferees are honest, but do not work when some conferees are malicious and attempt to delay or destruct the conference. Recently, Tzeng proposed a conference key agreement protocol with fault tolerance in terms that a common secret conference key among honest conferees can be established even if malicious conferees exist. In the case where a conferee can broadcast different messages in different subnetworks, Tzeng's protocol is vulnerable to a "different key attack" from malicious conferees. In addition, Tzeng's protocol requires each conferee to broadcast to the rest of the group and receive n 1 messages in a single round (where n stands for the number of conferees). Moreover, it has to handle n simultaneous broadcasts in one round. In this paper, we propose a novel fault- tolerant conference key agreement protocol, in which each conferee only needs to send one message to a "semitrusted" conference bridge and receive one broadcast message. Our SKNCOE, Department of Computer Engineering 2022-23 13 protocol is an identity-based key agreement, built on elliptic curve cryptography. It is resistant to the different key attack from malicious conferees and needs less communication cost than Tzeng's protocol.

"Identity-based key agreement protocol employing a symmetric balanced incomplete block design" Key agreement protocol is a fundamental protocol in cryptography whereby two or more participants can agree on a common conference key in order to communicate securely among themselves. In this situation, the participants can securely send and receive messages with each other. An adversary not having access to the conference key will not be able to decrypt the messages. In this paper, we propose a novel identity-based authenticated multi user key agreement protocol employing a symmetric balanced incomplete block design. Our protocol is built on elliptic curve cryptography and takes advantage of a kind of bilinear map called Weil pairing. The protocol presented can provide an identification (ID)- based authentication service and resist different key attacks. Furthermore, our protocol is efficient and needs only two rounds for generating acommon conference key.

## III. PROPOSED WORK/SYSTEM

The proposed system will be designed with the potential of serving as a decision support system based on facial features from video frames to determine the level of depression. The proposed project aims to develop a blockchain-based solution for managing the agri-food supply chain. With the increasing concerns about food safety, traceability, and sustainability, there's a critical need for a transparent and efficient supply chain management system in the agriculture and food industry.




The following Key features :

A. Decentralize and Management:

Utilize blockchain technology to create a decentralized ledger for recording transactions and data related tothe agri-food supply chain.

B. Smart Contacts:

Implement smart contracts to automate various processes such as payment settlements, quality assurance checks, and compliance verification.

C. Product Treceability:

Assign unique identifiers (such as QR codes or RFID tags) to each batch of agricultural productsand link them to corresponding blockchain records.

## IV. RESULT AND DISCUSSIONS

The results and discussions of a blockchain-based agri-food supply chain project typically revolve around evaluating the effectiveness, efficiency, and potential impact of implementing blockchain technology in the agricultural and food supply chain. The results and discussions of a blockchain- based agri-food supply chain project should provide insights into the tangible benefits, challenges, and future prospects of leveraging blockchain technology to transform the way agricultural products are produced, processed, and distributed.

## V. CONCLUSION

Blockchain, supply chain industry has gained numerous benefits to grow and move towards decentralization and achieve a trustless environment for all processes. However, despite the trustless natureof blockchain, it is hard to fully maintain trust between the seller and buyer of the product. This is because the entities may act maliciously and the buyer can doubt their credibility. Moreover, supply chain involves multiple processes and sub-processes that need to be carried out in a decentralized manner in order to achieve traceability, accountability and security.

## REFERENCES

[1] Chen, T. Xiang, Y. Yang, and S. S. M. Chow, “Secure cloud storage meets with secure network coding,” in IEEE INFOCOM, 2014, pp. 673–681.

[2] D. He, S. Zeadally, and L. Wu, “Certificateless public auditing scheme for cloudassisted wireless bodyarea networks,” IEEE Systems Journal, pp. 1–10, 2015

[3] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[4] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, “An efficient rfid authentication protocol providing strong privacy and security,” Journal of Internet Technology, vol. 17, no. 3, p. 2,2016.

[5] Patil, A., Rana, D., Vichare, S., & Raut, C. (2018). Effective Authentication for Restricing Unauthorized User. 2018 International Conference on Smart City and Emerging Technology (ICSCET). doi:10.1109/icscet.2018.8537323.